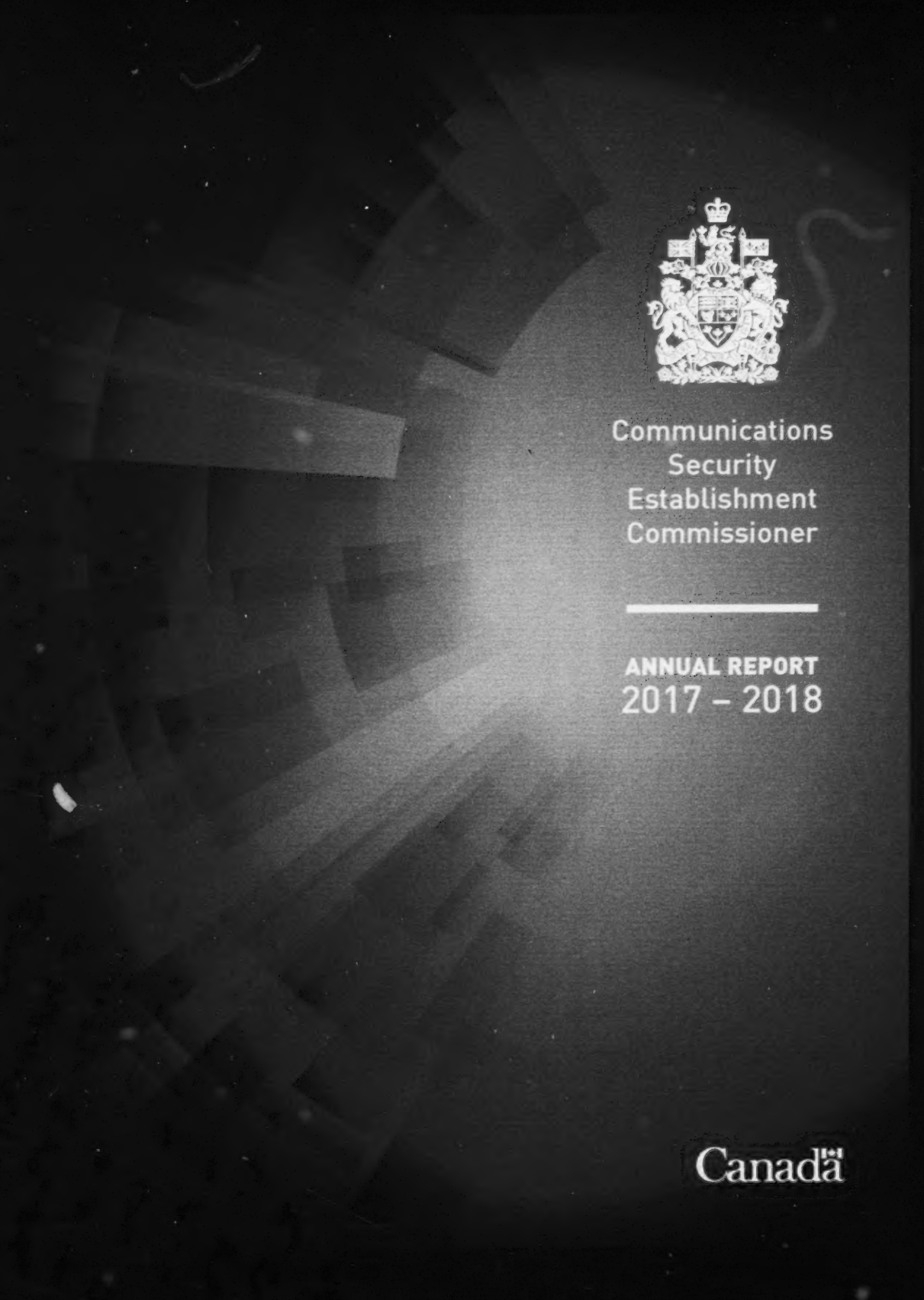

Communications Security Establishment Commissioner

ANNUAL REPORT
2017 – 2018

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1474, Station "B"
Ottawa ON K1P 5P6

Tel.: 613-992-3044
Fax: 613-992-4096
Website: www.ocsec-bccst.gc.ca

© Her Majesty the Queen in Right of Canada as represented by the
Office of the Communications Security Establishment Commissioner, 2018

Catalogue No. D95E-PDF
ISSN 1700-0874

Communications Security
Establishment Commissioner

The Honourable Jean-Pierre Plouffe, CD

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Jean-Pierre Plouffe, CD

June 2018

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa ON K1A 0K2

Dear Minister:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my annual report on my activities and findings for the period of April 1, 2017, to March 31, 2018, for your submission to Parliament.

Jean-Pierre Plouffe

P.O. Box/C.P. 1474, Station "B"/Succursale « B »
Ottawa ON Canada K1P 5P6

TABLE OF CONTENTS

Commissioner's Message 3

Commissioner's Mandate and Review Work 6

Update on CSE Efforts to Address Recommendations 9

Overview of 2017–2018 Findings and Recommendations 12

Highlights of Reports Submitted to the Minister in 2017–2018 14

1. Review of CSE's Authorities and Participation in a Multilateral Operational Initiative 14
2. Study of CSE's Operational Use of Internal Social Media-Type Platforms 18
3. Annual Review of CSE Disclosures of Canadian Identity Information, 2015–2016 22
4. Annual Review of CSE Disclosures of Canadian Identity Information, 2016–2017 26
5. Annual Review of CSE Cyber Defence Activities Conducted Under Ministerial Authorization, 2016–2017 28
6. Annual Combined Review of CSE Foreign Signals Intelligence Ministerial Authorizations, 2016–2017 and 2017–2018, and a One-End Canadian Communications Spot Check 34
7. Annual Review of Privacy Incidents and Minor Procedural Errors Files .. 41

Complaints About CSE Activities 44

Duty Under the *Security of Information Act* 44

Activities of the Office 44

Work Plan – Reviews Under Way and Planned 48

Annex A: Biography of the Honourable Jean-Pierre Plouffe, CD 49

Annex B: Excerpts from the *National Defence Act* and the *Security of Information Act* Related to the Commissioner's Mandate 50

COMMISSIONER'S MESSAGE

As I approach the end of my second term, I look back on a very active and satisfying year. I am privileged to be the Communications Security Establishment Commissioner at this critical juncture as the government overhauls the national security accountability framework.

First, Bill C-22 established the National Security and Intelligence Committee of Parliamentarians. As this bill received Royal Assent in June 2017, Bill C-59 was introduced, providing new authorities to security and intelligence agencies to meet an evolving threat and protect Canada and Canadians while at the same time broadening scrutiny overall. All of us in the review field affected by this legislation and this bill must strive to ensure that they do indeed strengthen the accountability of Canada's security and intelligence agencies. An inherent dimension of this accountability will be to ensure that we also continue to be as transparent as possible so that the public better understands how and with what degree of rigour those agencies, which must operate largely in secret, are being held accountable. The scope of the changes we are undergoing may seem daunting; however, a steady and committed approach as we proceed through the initial period will help achieve the desired objectives ultimately determined by Parliament.

Bill C-59 is complex and far-reaching in its scope. It proposes to make the most significant changes to national security laws, activities and accountability mechanisms since the *Canadian Security Intelligence Service Act* was enacted almost 35 years ago, creating the Security Intelligence Review Committee and the Inspector General. Bill C-59 will establish three new acts and amend five existing ones. My current role of reviewing past activities of CSE will be assumed by a new, single review body, the National Security and Intelligence Review Agency that will be mandated to review any national security activities carried out by any government agency or department. Another law created by this bill, the Intelligence Commissioner Act, will see my office transition to a new, quasi-judicial role. I will be involved in the decision-making process, reviewing ministerial authorizations concerning certain activities of CSE and the Canadian Security Intelligence Service (CSIS). If I am satisfied after my review that the authorizations signed by the minister are reasonable, I will, as Intelligence Commissioner, have the authority to approve them, and only then could the activities be undertaken.

I am watching the bill's progress through Parliament with great interest. To the extent possible, I want to ensure that the proposed legislation does not recreate the problems that have troubled Part V.1 of the *National Defence Act*. Introduced in 2001, Part V.1 contained ambiguities that, despite recommendations issued repeatedly by my predecessors and me, were never addressed, until now with Bill C-59. However, this bill contains ambiguities of its own. To this end, I made several submissions to the House of Commons Standing Committee on Public Safety and National Security (SECU) that was examining Bill C-59. I outlined proposed amendments to provide clarity and avoid ambiguities. Other amendments I proposed would, I believe, add a degree of flexibility with the goal of increasing the efficiency of the process of the Intelligence Commissioner's review and approval of certain ministerial authorizations for CSE and CSIS.

Canada isn't alone in making major changes to its national security authorities and accountability mechanisms. Other countries have also been responding to demands for new tools to counter ever-evolving threats and at the same time strengthening accountability. The close partnership of the intelligence agencies in Canada, the United States, the United Kingdom, Australia and New Zealand (the Five Eyes) provided an ideal springboard for a forum for officials from the review and oversight bodies of these countries to explore mutual issues and concerns and to share best practices. With my colleague the Chair of the Security Intelligence Review Committee and our counterparts from these countries, we agreed to establish the Five Eyes Intelligence Oversight and Review Council in late 2016. Canada hosted the first in-person meeting of the Council at my offices in October 2017. The Intelligence Commissioner would continue to participate in this group.

This council is just one part, though a significant one, of efforts to enhance exchanges with review and oversight bodies in other countries. Discussions within this group can contribute to the effectiveness of the important work that intelligence agencies do while ensuring that such work is done within their legal authorities, including respecting privacy rights within our respective countries.

Before closing, I would like to offer my congratulations to Ms. Greta Bossenmaier on her appointment as National Security and Intelligence Advisor to the Prime Minister. As Chief of CSE, I appreciated her professional, frank and cooperative approach to our working relationship.

Finally, I would like to end with a word to commend my staff for their superb and unrelenting efforts during this past dynamic year: in assessing Bill C-59 and ensuring our contribution was and is positive and constructive; in diligently beginning preparations for the transition to a new and unique oversight role in Canada; in planning for the impact of this transition on the internal services of my office and the many additional responsibilities implied; in ensuring a constructive dialogue with CSE and CSIS with regard to the new role for the proposed Intelligence Commissioner; and all the while upholding our ongoing

responsibilities of reviewing the activities of CSE to ensure it is complying with the law and protecting the privacy of Canadians, until such time as Bill C-59 becomes law.

COMMISSIONER'S MANDATE AND REVIEW WORK

The Office of the Communications Security Establishment (CSE) Commissioner is an independent review body.

MANDATE

The CSE Commissioner's mandate is set out under Part V.1 of the *National Defence Act* (NDA):

1. to review activities of CSE – which includes foreign signals intelligence and information technology (IT) security activities to support the Government of Canada – to determine whether they comply with the law;
2. to undertake any investigation the Commissioner considers necessary in response to a written complaint; and
3. to inform the Minister of National Defence (who is accountable to Parliament for CSE) and the Attorney General of Canada of any CSE activity that the Commissioner believes may not be in compliance with the law.

Under section 15 of the *Security of Information Act*, the Commissioner also has a mandate to receive information from persons who are permanently bound to secrecy if they believe it is in the public interest to release special operational information of CSE.

The *National Defence Act* requires that the CSE Commissioner be a supernumerary or retired judge of a superior court. The *National Defence Act* provides the Commissioner with full independence, as well as full access to all CSE facilities and systems, and full access to CSE personnel, including the power of subpoena to compel individuals to answer questions. The Commissioner has a separate budget granted by Parliament.

CONSIDERATIONS IN A REVIEW

The Commissioner's approach to reviews is both purposive – based on his mandate – and preventive. CSE activities include collecting foreign signals intelligence on foreign targets located outside Canada, that is, information about the capabilities, intentions or activities of foreign targets relating to international affairs, defence or security. CSE is also Canada's lead technical agency for cyber defence and for the cryptography and other technologies needed to protect government computer systems and networks containing sensitive national and personal information. CSE also has a mandate to use its unique capabilities to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

CSE's activities are distinct from security and criminal intelligence that is collected by other agencies, which is information on activities that could threaten the security of Canada or public safety and is usually acquired from targeting Canadians under various lawful authorities. CSE activities are specifically prohibited from being directed at Canadians or persons in Canada. Restricting intelligence gathering to foreign targets outside Canada is complicated by the interconnected and ever-evolving global information infrastructure, as well as by the foreign targets, who are themselves technologically astute. CSE requires sophisticated technical capabilities to acquire and analyze information and to detect and mitigate malicious cyber activity. CSE's methods are effective only if they remain secret.

In this challenging environment, reviewers need specialized knowledge and expertise to understand the many technical, legal and privacy aspects of CSE activities. They also require security clearances at the level necessary to examine CSE records and systems. Reviewers are bound by the *Security of Information Act* and cannot divulge to unauthorized persons the sensitive information they access.

After an activity is selected for review, the activity is assessed against the following standard set of criteria:

- **Legal requirements**: the Commissioner expects CSE to conduct its activities in accordance with the *Canadian Charter of Rights and Freedoms*, the *National Defence Act*, the *Privacy Act*, the *Criminal Code*, and any other relevant legislation.
- **Ministerial requirements**: the Commissioner expects CSE to conduct its activities in accordance with ministerial direction, following all requirements and limitations set out in a ministerial authorization or directive.
- **Policies and procedures**: the Commissioner expects CSE to have appropriate policies and procedures in place to guide its activities and to provide sufficient direction on legal and ministerial requirements including the protection of the privacy of Canadians. He expects CSE employees to be knowledgeable about and comply with policies and procedures. He also expects CSE to have an effective compliance validation framework to ensure the integrity of operational activities is maintained, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

REPORTING ON FINDINGS

Classified report on each review to the Minister: The results of individual reviews are produced as classified reports to the Minister that document CSE activities, contain findings relating to the standard criteria, and disclose the nature and

significance of any deviations from the criteria. If necessary, the Commissioner makes recommendations to the Minister aimed at improving privacy protections or correcting problems with CSE operational activities raised during the course of review. Following the standard audit practice of disclosure, CSE is provided with draft versions of reports to confirm factual accuracy. The findings and conclusions are free of any interference by CSE or any Minister.

Public reports annually to Parliament: The Commissioner's annual report is a public document provided to the Minister, who by law must table it in Parliament. The Commissioner's office publishes the titles of all review reports submitted to the Minister – 114 to date – on its website.

OFFICE RESOURCES

In 2017–2018, the Commissioner was supported by 11 full-time positions, together with a number of subject matter experts, as required. The office's expenditures were $1,967,061, which is within the overall funding approved by Parliament. The office provides more detail on its expenditures on its website.

UPDATE ON CSE EFFORTS TO ADDRESS RECOMMENDATIONS

CSE has accepted and implemented, or is working to address, 95 percent (161) of the 170 recommendations made since 1997, including the four recommendations in reports this year. Commissioners track how CSE addresses recommendations and responds to negative findings as well as areas for follow-up identified in reviews. The Commissioner is monitoring nine recommendations that CSE is working to address – six outstanding recommendations from previous years and three from this year.

This past year, CSE advised the office that work had been completed in response to 11 past recommendations. CSE has already addressed one recommendation from this year.

In the Commissioner's 2008–2009 annual report, Commissioner Gonthier reported on his review of CSE activities, conducted under a ministerial directive, in support of its foreign signals intelligence collection mandate. In this review, he recommended that CSE reconcile certain discrepancies between ministerial expectations and its own practices. He also recommended that CSE review, update and finalize key policy documents respecting these activities, and that it clarify certain terms used in the documents. CSE approved an updated version of the relevant operational policy in May 2017 to clarify guidelines pertaining to the program.

In the 2015–2016 cyber defence ministerial authorization review, the Commissioner recommended that CSE promulgate guidance on the consistent annotation and counting of what constitutes a cyber defence private communication. CSE has implemented new guidance and training, as well as instituted upgrades to automate the identification of potential private communications and standardize the counting of cyber defence private communications.

CSE has also taken steps to respond to the Commissioner's recommendation from the review of a specific CSE foreign signals intelligence method of collection conducted under ministerial authorization (summarized in the 2015–2016 annual report). The Commissioner recommended that CSE reconcile the discrepancies between its practices and the administrative requirements in the ministerial directive. In September 2017, CSE introduced a foreign signals intelligence operational risk framework that establishes a risk assessment process that considers legal, reputational, partnership and operational risks associated with foreign signals intelligence operations. The collection program now has comprehensive procedures that are accessible to all staff that may be required to engage in activities in support of that program.

In last year's review of CSE information sharing with foreign entities, the Commissioner made three recommendations, two of which CSE fulfilled in July 2017.

In response to the recommendation that caveats be applied consistently to all exchanges between CSE and foreign entities and that CSE use appropriate systems to keep a record of all information released, CSE standardized the process of information sharing with foreign entities. In response to the recommendation that CSE issue overarching policy guidance for information exchanges with foreign entities, CSE issued guidelines that incorporate the foreign signals intelligence operational risk framework, as well as new policy.

In last year's review of CSE's foreign signals intelligence activities conducted under ministerial authorization, the Commissioner recommended that CSE reporting to the Minister on private communications describe the private communications better and explain the extent of privacy invasion. Certain communications technology were creating a distorted view of the number of Canadians or persons in Canada that are involved in (i.e., are the other end of) these CSE interceptions. For the first time this year, CSE reported additional information to the Minister explaining the reason for the substantial increase in the number of recognized private communications.

Another recommendation CSE addressed from the Commissioner's 2016–2017 annual report pertained to intercepted solicitor-client privileged communications. CSE modified its policy to describe what is expected of CSE employees when handling solicitor-client communications collected under CSE's foreign signals intelligence mandate.

CSE has also responded to one recommendation made this year in the office's review of 2015–2016 CSE disclosures of Canadian identity information. In that review, the Commissioner recommended that CSE take measures to ensure that all requests for the release of suppressed Canadian identity information stipulate both the lawful authority under which the information is being requested and a robust operational justification of the need to acquire that information, consistent with the requesting agency's mandate. CSE has adjusted its processes to ensure that the requesting agency's legal authority is explicit and the operational justification is robust and clear before CSE considers the disclosure of Canadian identity information.

Finally, the Commissioner recommended, in two past reviews, that amendments be made to the ***National Defence Act***. In the office's review of CSE information technology security activities conducted under ministerial authorization (reported in the Commissioner's 2014–2015 annual report), the Commissioner recommended that subsection 273.65(3) of the ***National Defence Act*** be amended to remove any ambiguities respecting CSE's authority to conduct information technology security activities that risk the interception of private communications. Also, as a result of a review of CSE foreign signals intelligence metadata activities, where the Commissioner found that CSE had failed to minimize certain Canadian identity information prior to sharing it with CSE's Second Party partners,

the Commissioner recommended that the ***National Defence Act*** be amended to provide an explicit authority and a clear framework for CSE metadata activities. On June 20, 2017, the government tabled Bill C-59, an Act respecting national security matters. Part 3 of this Bill enacts the ***Communications Security Establishment Act***, which includes clarified provisions pertaining to information technology security authorities as well as provisions pertaining to authorities to collect and use metadata.

Legal interpretation issues have bedeviled this office since 2001 when CSE was first legislated following the terrorist attacks in the United States. Since then, past and present Commissioners have made various recommendations to amend the ***National Defence Act***. The Commissioner is pleased that the government has taken action that responds to these recommendations.

OVERVIEW OF 2017–2018 FINDINGS AND RECOMMENDATIONS

During the 2017–2018 reporting year, the Commissioner submitted eight classified reports to the Minister on his reviews of CSE activities.

The seven reviews, and one study, were conducted under the Commissioner's authority:

- to ensure CSE activities are in compliance with the law – as set out in paragraph 273.63(2)(a) of the ***National Defence Act***; and
- to ensure CSE activities carried out under a ministerial authorization are authorized – as set out in subsection 273.65(8) of the ***National Defence Act***.

The Commissioner's office reviewed a matter that had been identified as needing a separate examination, following last year's review of CSE's information sharing and relationships with foreign entities outside of the Five Eyes. The office reviewed CSE's authorities and participation in a multilateral operational initiative.

The Commissioner's office also completed a study of CSE's operational use of internal social media-type platforms to acquire detailed knowledge of these activities as well as to identify any issues that may require follow-up review.

As in previous years, the Commissioner conducted annual reviews of ministerial authorizations for foreign signals intelligence and cyber defence activities, including a spot check examination of one-end Canadian communications (including private communications) acquired, used, retained and destroyed by CSE, and of CSE incidents and procedural errors related to privacy. The office completed both the 2015–2016 and 2016–2017 reviews of CSE disclosures of Canadian identity information. The 2015–2016 review had carried over into this year.

THE RESULTS

Each year, the Commissioner provides an overall statement on findings about the lawfulness of CSE activities. ***This past year, all CSE activities reviewed complied with the law.***

As well, this year, the Commissioner made four recommendations to promote compliance with the law and strengthen privacy protection, including that:

1. in order to ensure clarity for any new activities involving information sharing with foreign entities, CSE conduct adequate assessments with respect to authorities and measures to protect the privacy of Canadians, prior to commencing the activity;
2. CSE take measures to ensure that all requests for the release of suppressed Canadian identity information stipulate both the lawful authority under which the

information is being requested and a robust operational justification of the need to acquire that information, consistent with the requesting agency's mandate;

3. CSE clarify the language in the ministerial authorizations to accurately reflect the legal protection recognized and afforded to solicitor-client communications in Canadian law, and ensure consistency with language in policy and with practice, in both CSE's information technology security and foreign signals intelligence activities; and
4. CSE ensure that future ministerial authorization request memoranda to the Minister contain comprehensive information to describe and document contemplated CSE foreign signals intelligence ministerial authorization activities in a thorough manner, to better support the Minister when making a decision.

HIGHLIGHTS OF REPORTS SUBMITTED TO THE MINISTER IN 2017–2018

1. Review of CSE's Authorities and Participation in a Multilateral Operational Initiative

BACKGROUND

During last year's review of CSE's information sharing with foreign entities, the Commissioner's office learned that CSE was participating in a multilateral operational initiative. Questions were raised about the authority under which CSE was participating, as well as about the guidance, policies and operating framework for CSE's participation. For these reasons, the Commissioner decided to examine this activity separately.

The review was an opportunity to acquire detailed knowledge with respect to CSE's participation in the multilateral initiative to determine whether the activities complied with Canadian law, and to ensure adequate measures were being taken to protect the privacy of Canadians. The office examined activities, reporting, guidance and policy documents, and internal correspondence related to the initiative for the November 2013 to June 2016 period.

CSE has had a long-standing multilateral relationship with a number of foreign entities that involves cooperation and information sharing on matters of mutual interest. A recent initiative by this multilateral group has been to collaborate on analytical products based on information shared by participants. To date, this initiative has been focused on the terrorism threat posed by extremist travellers, but there is potential for similar collaboration in support of other common interests.

Under this multilateral operational initiative, participants collaborate on analytical products. The information used for this analysis is contributed by individual participants, who acquire the information through their independent collection efforts under their respective legal mandates. Through participation in this initiative, CSE may access information shared by other participants, as well as the jointly produced analytical reporting.

CSE's collection mandate and limitations differ from that conferred by the legal and policy regimes of several other participants.

Under its foreign signals intelligence mandate, carried out pursuant to paragraph 273.64(1)(a) of the ***National Defence Act*** – part (a) of CSE's mandate – CSE cannot direct its activities at Canadians and such activities must be subject to

measures to protect the privacy of Canadians – paragraphs 273.64(2)(a) and (b). When CSE provides technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties, CSE is subject to any limitations imposed by law on these agencies, pursuant to paragraph 273.64(1)(c) of the ***National Defence Act*** – part (c) of CSE's mandate.

If the Canadian Security Intelligence Service requests assistance from CSE pursuant to part (c) of CSE's mandate, CSE may act as a secure conduit for information from a foreign entity that may relate to a threat to the security of Canada, but may have been acquired by directing activities at a Canadian.

FINDINGS AND RECOMMENDATION

At the outset of this review, the Commissioner's office questioned under what authority CSE was operating while participating in the multilateral initiative as it was not clear whether it was participating under its foreign signals intelligence mandate or its assistance mandate. The office sought confirmation from CSE as to what authority it was operating under. CSE maintains that prior to commencing the activity it had determined that CSE was participating in the initiative under its foreign signals intelligence mandate. However, internal documents examined by the Commissioner's office demonstrated there was discussion within CSE concerning the extent to which the different parts of its mandate applied, due to the possibility of CSE receiving information about Canadians or information that is the result of a participant directing activities at a Canadian, and how such instances would be managed. The Commissioner's office found no evidence of a decision having been made and CSE did not provide an explicit answer about which authority applied until later in the review.

Prior to participating in the multilateral initiative, and in the early stages of its participation, CSE did not adequately document its activities, nor did it institute corresponding measures with respect to the identified authority (i.e., CSE's foreign signals intelligence mandate) or put policy in place.

The Commissioner's office was informed that CSE did not obtain specific legal advice regarding its participation in this multilateral initiative, but it did consider legal advice on a related matter to provide guidance during the initial stages.

In response to questions from the Commissioner's office concerning the authority under which CSE was participating in the multilateral initiative, CSE obtained specific legal advice on the subject and shared it with the Commissioner's office.

Authority

The Commissioner found that in the early stages of this review CSE did not clearly express its approach to participating in the multilateral initiative. Instead of explicitly planning how to participate, CSE reacted to developments and concentrated

on managing the risk of receiving information obtained from activities directed at Canadians that was undertaken by participants under their sovereign authorities. It was only with the benefit of time, experience and hindsight that CSE determined the risk of receiving information relating to Canadians was low.

By participating in the multilateral initiative under its foreign signals intelligence mandate, as for any foreign signals intelligence activities, CSE could not receive information derived from the targeting of a Canadian and could not direct its activities at Canadians; such activities would also have to be subject to measures to protect the privacy of Canadians.

Each participant in the multilateral initiative operates under its own legal and policy framework. It is therefore possible that a participant may choose to direct collection activities against a Canadian, should it be in its national interests to do so. When participants choose to share information, they usually do so without revealing the source of that information and there are no means to identify how the information being shared was acquired. Thus, there is a possibility that information provided by the participants for the counter-terrorism mission could include information that is the result of directing collection activities at a Canadian.

The Commissioner found that the mutually agreed upon privacy protection measures put in place for this multilateral initiative were unsatisfactory, as they did not sufficiently address the potential for CSE to unknowingly receive information that may have been sourced from another participant directing collection activities against a Canadian under its own national legal and policy framework. However, based on the information reviewed, the Commissioner found no evidence of non-compliance with the law. The Commissioner's office examined all of the reports produced by the multilateral initiative during the period under review and found no instances of information from participants that involved Canadians.

While the initial concept of the multilateral initiative was signals intelligence agencies collaborating on counter-terrorism projects, the stated intent was also to be open to responding to other crises or threats. However, the focus continues to be on extremist travellers. In concentrating on this, notwithstanding the low risk, there remains a possibility that CSE may unknowingly receive information derived by another participant directing collection activities against a Canadian under its own domestic legal and policy framework.

EXTREMIST TRAVELLERS

An extremist traveller (also known as a "foreign fighter") can be defined as an individual who is suspected of travelling abroad to engage in terrorism-related activity, for example, women and men who have left Canada to join the terrorist group calling itself the Islamic State.

Guidance

It is positive that based on the information examined there were adequate guidance and policy documents on what non-Canadian information CSE may share with other participants and how to do so. These documents make clear that CSE will not provide information relating to a Canadian. The Commissioner has no concerns with respect to what CSE shares with the other participants.

CSE also put certain measures in place to protect the privacy of Canadians in the use of information received from the multilateral initiative. CSE analyzes data received from the initiative and if it is determined to be of value, reports and disseminates it. If required, CSE will suppress any Canadian identity information in the report as a measure to protect the privacy of Canadians.

However, while CSE has policy in place regarding activities conducted under its foreign signals intelligence mandate, the Commissioner found a lack of specific policy and guidance for CSE participation in this particular multilateral initiative with respect to the possibility of receiving information obtained from activities directed at Canadians. Guidance to CSE employees was informal and focused on efforts to avoid exposure to situations that may involve other participants directing activities at a Canadian. Information examined by the Commissioner's office suggested that CSE planned to provide documentation to other participants in the initiative to clarify CSE's legal and policy limitations. CSE was unable to provide a record to demonstrate that this was done. During the latter stages of the review, CSE sent correspondence to the other participants in the multilateral initiative to clarify CSE's legal and policy guidelines, specifically reiterating the limitations of part (a) of CSE's mandate and restrictions relating to the receipt of information acquired from activities directed against Canadians.

Last year, while conducting the review of information sharing with foreign entities, which initially raised questions concerning CSE's participation in this multilateral initiative, the Commissioner found that formal agreements with certain foreign entities refer only in broad terms to measures to protect the privacy of Canadians rather than explicitly state CSE legal authorities and restrictions, including the stipulation that under its foreign signals intelligence mandate CSE cannot receive information derived from directing activities at a Canadian. CSE responded

positively to these findings during the review and provided letters to these foreign entities, describing CSE's legal authorities and restrictions as an interim measure pending changes to the agreements. The Commissioner was satisfied with this approach; however, he encouraged CSE to quickly conclude and/or amend all agreements with foreign entities at the earliest opportunity, as recommended in last year's review of information sharing with foreign entities.

Further, the Commissioner **recommended** that, to ensure clarity for any new activities involving information sharing with foreign entities, CSE conduct adequate assessments with respect to authorities and measures to protect the privacy of Canadians prior to commencing the activity.

CONCLUSION

Based on the information reviewed, the Commissioner found no evidence of non-compliance with the law. The Commissioner understands that CSE's participation in the multilateral initiative fulfills a top Government of Canada priority of protecting Canadians from the threat of terrorism. However, it is also necessary to ensure that foreign entities CSE interacts with understand the legal limitations under which CSE operates. Therefore, as a result of this review, the Commissioner will closely monitor the implementation of the recommendation from last year's review of information sharing with foreign entities, as well as the recommendation in this report.

2. Study of CSE's Operational Use of Internal Social Media-Type Platforms

BACKGROUND

The Commissioner's office conducted a study of CSE's operational use of internal social media-type platforms from January 1, 2016, to July 31, 2017. CSE has increased its use of such platforms in recent years, primarily to enrich the sharing of operational information and ideas both internally and among the agency's partners.

While benefiting CSE and its partners, the use of these platforms was seen to have potential implications for the privacy of Canadians and compliance with the law. Accordingly, the Commissioner's office undertook this study to familiarize itself with how CSE uses internal social media-type platforms in an operational context so as to better understand and assess the potential impacts on privacy, as well as any issues with respect to lawfulness, and thus inform the Commissioner. The Commissioner's office also sought to use the acquired knowledge to help identify

matters that may require follow-up review, as well as to inform future reviews in general. The study was conducted under the authority of the Commissioner as articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act*.

CSE's internal social media-type platforms include virtual workspaces, or groups, which are set up to allow designated participants to access specific information repositories. Some of the groups are strictly internal to CSE, while others, known as externally accessible groups, include participants from other domestic and/or foreign organizations. There is no relationship or link between these internal social media-type platforms used by CSE for information-sharing purposes and social media tools used by the public.

CSE'S INTERNAL SOCIAL MEDIA-TYPE PLATFORM

CSE has adopted a collaborative business platform for mission operations (foreign signals intelligence and information technology security) that provides a means through which operational personnel can participate in communities of interest, share information, and collaborate on operations and mission-related projects. The ultimate objective is the production of high-quality, timely and useful intelligence products through collaboration within CSE and with its Five Eyes and Canadian security and intelligence partners.

OBSERVATIONS

Policies and controls

CSE has policy and written guidance for the use of internal social media-type platforms. It addresses, among other matters, privacy and lawfulness, and supplements other CSE operational policy that has a broader application. Activities involving the use of internal social media-type platforms must be compliant with all applicable operational policy. This includes the retention, use and sharing of Canadian identity information. With only limited exceptions, sharing of Canadian identity information should exclude Second Party participants and domestic partner agencies. During the period of study, no Canadian identity information was shared via these platforms with any foreign entities or with domestic partner agencies.

CSE has also developed an approval and compliance monitoring regime respecting the use of these platforms, which involves operational line managers and internal review teams dedicated to ensuring appropriate approvals, access, content, data sharing and retention, as well as training.

Privacy culture and awareness

A CSE culture of respecting privacy is reflected in the privacy awareness and practices displayed by the CSE presenters and interviewees during the course of this study, including in demonstrations of the platform and the treatment of any Canadian identity information contained within it. This ethos is also reflected in the policy instruments and guidance that has been developed and promulgated specifically for operational use of internal social media-type platforms, the access requirements and limitations built into these platforms, the logging and tracking of platform usage, and the compliance monitoring and reporting regimes that are in place.

Training

Training on the use of CSE's internal social media-type platforms is provided to CSE employees and, where applicable, external participants. This training appears to be adequate; however, an internal CSE review conducted in 2017 revealed that less than half of externally accessible group owners had undergone the required training. The office was advised that CSE is addressing this matter.

Internal compliance assurance and information management

Compliance teams in CSE's SIGINT and IT Security branches monitor the use of CSE's internal social media-type platforms for compliance with CSE policies, authorities and direction. For example, during the period of this study, CSE's IT Security Compliance team undertook to verify that unassessed cyber defence data, which is not permitted on internal social media-type platforms, was not accessible on these platforms. As a result, one instance of unassessed data was discovered, prompting the compliance team to reiterate the policy by issuing a communiqué on the acceptable use of such platforms.

The SIGINT Compliance team also undertook two reviews during the same period. While the internal reviews raised no concerns about content or privacy, the team found that 19 percent of active externally accessible groups had not properly documented the approvals they needed to be established and that several changes of externally accessible group ownership had not been reported as required. The compliance team recommended that approvals and ownership changes be documented centrally and consistently for compliance monitoring and review purposes. (The SIGINT Compliance team also made a recommendation regarding the above-noted training gap.) CSE has advised that these recommendations have been accepted and implemented.

As part of the compliance monitoring process, SIGINT managers verify each year that all holdings of Canadian identity information – including internal social media-type platforms – are valid and continue to be required. In the context of this study, the Commissioner's office found inconsistencies in how the forms were

being completed. The office also observed that, as of November 2017, the most recently submitted forms were dated July 2016. The Commissioner's office would expect the SIGINT branch to have reviewed its information repositories since then to be compliant with its own policy. CSE has advised that the compliance review for 2017 respecting Canadian identity information commenced in November of that year and that corrective action has been taken.

An internal social media group had been set up to assist with a high-priority operational matter. After the case was successfully concluded, the internal social media group, which contained Canadian privacy-related information, remained open and accessible to all CSE operational personnel with accounts on this platform for more than 15 months. CSE explained the usefulness of having this particular group remain open; however, the Commissioner's office questions the need for it to be active for so long after the conclusion of the operation and for such potentially sensitive information to remain so widely accessible. CSE policy dictates that information in internal social media-type platforms is considered transitory and, when no longer needed – particularly any retained Canadian identity information or other Canadian privacy-related information – must be deleted. As per CSE policy, information deemed to be of operational value should be saved in CSE's official corporate repository.

CSE has issued direction on records management within the context of internal social media-type platforms, as well as more generally. Yet, in conducting this study, the Commissioner's office examined documents constituting CSE official policy instruments that did not specify an effective date (or any date) or provide an indication of being an official record. Although CSE advised that these policy instruments are accessible to those who require them, it is important to recognize that the clarity offered by such information aids operations by facilitating version control and helping to ensure that mission personnel receive current and unambiguous direction. Scrupulous records management is also crucial to effective compliance monitoring, auditing and review.

CONCLUSION

This study concluded that CSE has a satisfactory policy suite in place governing the operational use of internal social media-type platforms, although some CSE written policy direction that was reviewed did not specify an effective date or provide a clear indication that it constituted an official record. This can detract from its effectiveness in providing clear, unambiguous direction to employees and allowing effective compliance monitoring, auditing and review. Also, CSE promotes a culture of compliance regarding privacy protection in the use of internal social media-type platforms and, except for a gap in the training of certain users, the training scheme for its users appears to be adequate, as CSE employees are knowledgeable and conscientious with respect to protecting the privacy of

Canadians in the operational use of such platforms. The Commissioner will monitor issues identified in this study and determine whether follow-up review for any of them is warranted.

3. Annual Review of CSE Disclosures of Canadian Identity Information, 2015–2016

BACKGROUND

The Commissioner's office annually reviews a sample of CSE disclosures of Canadian identity information – which includes any information uniquely relating to and that may identify a Canadian. This review of disclosures during 2015–2016 was completed after March 31, 2017, and therefore is being reported this year. The objective of the review was to verify that CSE, in its disclosures of Canadian identity information, complied with the law, ministerial direction, and its policies and procedures, including assessing the extent to which it protected the privacy of Canadians.

Under its foreign signals intelligence mandate, CSE is "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence" (paragraph 273.64(1)(a) of the ***National Defence Act***). These activities shall not be directed at Canadians or persons in Canada and the use and retention of intercepted information shall be subject to measures to protect the privacy of Canadians (paragraphs 273.64(2)(a) and (b) of the ***National Defence Act***).

While the ***National Defence Act*** does not provide an explicit authority for CSE to disclose Canadian identity information, including personal information, it is understood that this authority is implied in CSE's foreign signals intelligence mandate. Commissioners, including the current Commissioner, have recommended that the ***National Defence Act*** be amended to provide an explicit authority for CSE to collect, use and disclose information about Canadians collected incidentally to its mandated activities. (This now seems to have been addressed in the government's proposed legislation, Bill C-59, An Act respecting national security matters.)

In the process of collecting foreign signals intelligence in support of the Government of Canada's intelligence priorities, CSE may unintentionally acquire Canadian identity information or information about Canadians. If the information is used in a report, any Canadian identity information – including names, phone numbers, Internet protocol addresses, passport numbers and any other information that may reveal the identity of a Canadian person or corporation – must be suppressed by using generic references. As well, CSE foreign intelligence reports can include references to Canadians only if it is necessary to understand the foreign intelligence.

When CSE produces a foreign intelligence report that includes suppressed Canadian identity information, CSE clients who can demonstrate they have the legal authority and the operational justification to receive the Canadian identity information may submit a request for the disclosure of the information. After assessment, CSE may release the Canadian identity information to a client under paragraph 273.64(1)(a) of the ***National Defence Act*** and, for personal information, consistent with subsection 8(2) of the ***Privacy Act***.

CSE's authority to disclose suppressed Canadian identity information is dependent on the client's authority to collect this Canadian identity information. The disclosure of Canadian identity information must be done in compliance with the ***National Defence Act*** and the ***Privacy Act*** and in compliance with CSE's own operational policy framework, which recognizes that the receiving client must justify its right to receive the information. When personal information is to be disclosed, CSE must be satisfied that the requesting client is collecting the information for the purposes related directly to an operating program or activity for which the client is responsible (section 4 of the ***Privacy Act***) and that the information is being requested for a foreign intelligence purpose in accordance with Government of Canada intelligence priorities or for a consistent purpose. If the request for disclosure of the suppressed Canadian identity information does not fall within the scope of the foreign signals intelligence mandate, there are other circumstances described in section 8(2) of the ***Privacy Act*** that would permit such a disclosure.

For this review, the Commissioner's office selected and examined a sample of approximately 20 percent (initially 243 requests) of the 1,211 requests from CSE's Government of Canada clients for disclosure of Canadian identity information contained in CSE reports.

The requests examined were received by CSE from July 1, 2015, to June 30, 2016. All government institutions that made a request for Canadian identity information during that period were represented in the sample. When it became clear that a particular Government of Canada client was submitting requests that contained insufficient details, the sample was expanded to 249 requests to include all 27 requests submitted by that client.

The office also examined all 100 requests from Second Party partners and the 5 requests made by a Government of Canada client to share specified Canadian identity information with non-Five Eyes entities. CSE is responsible for conducting a mistreatment risk assessment when it releases the information; however, other Government of Canada institutions continue to be responsible for conducting a mistreatment risk assessment when the information is being released via their own channels. In disclosures involving non-Five Eyes recipients, CSE includes a specific caveat to remind the requesting government client of its responsibility to conduct an assessment of the risks in sharing information with a foreign entity.

CSE'S FIVE EYES PARTNERS

The Five Eyes partners are CSE and its main international partner agencies in the Five Eyes countries: the United States' National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Signals Directorate and New Zealand's Government Communications Security Bureau. They are also known to each other as Second Party partners.

Counts of disclosures of Canadian identity information are based on CSE's method of counting. The number of requests represents the number of instances that institutions or partners submitted separate requests for disclosure of identity information suppressed in reports, providing a unique operational justification in each case. One request may involve multiple Canadian identities, and one Canadian identity may be disclosed multiple times to different institutions or partners.

FINDINGS AND RECOMMENDATION

The Commissioner was satisfied that CSE disclosures of Canadian identity information – including those to Second Party partners or involving a Government of Canada client disclosure to a non-Five Eyes entity – complied with the law and with ministerial direction concerning the protection of the privacy of Canadians.

CSE made one technical change to upgrade the system used to process Government of Canada client requests for Canadian identity information; this system now includes the original request on denied disclosure requests – information that was previously not included.

In how CSE discloses Canadian identity information to Government of Canada clients, the Commissioner noted an opportunity for CSE to strengthen its procedures so that it exercises a higher degree of diligence when considering the operational justification provided. This approach would contribute to the application of satisfactory measures by CSE to protect Canadian identity information and the privacy of Canadians in accordance with the *National Defence Act* and the *Privacy Act*.

After examining relevant documentation, the Commissioner's office raised concerns with CSE policy staff and managers, senior CSE officials, and Justice Canada's legal counsel at CSE about eight requests from the same client that were missing explicit statements of specific authorities and operational justifications. Although the Commissioner determined that the Government of Canada client did have the legal authority to collect Canadian identity information in these cases, CSE disclosed the information without obtaining sufficient detail from the client to substantiate the client's legal authority to collect Canadian identity

information, nor an adequate operational justification demonstrating that the client's collection of Canadian identity information related directly to an operating program. The Commissioner found that CSE's disclosure process lacked rigour and that CSE did not exercise sufficient diligence in these cases. CSE policy does not require a client to provide a specific statute as an authority to receive information – it is sufficient that the client provide a robust justification for its request that outlines the client's requirement for the suppressed information; identifies how the information relates to its mandate and operational program; and confirms that the information will remain under the control of the requestor.

CSE acknowledged that the justifications originally submitted by the client did not provide adequate details.

The Commissioner **recommended** that CSE take measures to ensure that all requests for the release of suppressed Canadian identity information stipulate both the lawful authority under which the information is being requested and a robust operational justification of the need to acquire that information, consistent with the requesting agency's mandate. The Commissioner expects to see evidence of CSE's action on this recommendation in its review of disclosures of Canadian identity information for 2017–2018.

CONCLUSION

In response to the issues identified in this review, CSE has already instructed the team responsible for the disclosures of Canadian identity information to ensure additional scrutiny of future requests. CSE also temporarily suspended, except in emergencies, disclosures to the Government of Canada client that had submitted requests containing insufficient details. CSE subsequently adjusted its procedures so that it exercises a higher degree of diligence when considering the justifications provided by this Government of Canada client for Canadian identity information and is re-examining the information requirements that clients must provide to request Canadian identity information. Finally, CSE changed its process to require a higher approval level for requests for Canadian identity information from this particular Government of Canada client. These are welcome developments.

Approval levels were the subject of some policy amendments that CSE has made since the 2014–2015 review. CSE lowered the approval level required to authorize the disclosure of Canadian identity information in three other specific circumstances. According to CSE, this addressed an issue of unnecessarily high approval authorities that were delaying the release of information to CSE clients. Impacts of these policy changes were unnoticeable. However, the Commissioner will monitor this change in future reviews.

4. Annual Review of CSE Disclosures of Canadian Identity Information, 2016–2017

BACKGROUND

This is the ninth consecutive annual review of a sample of CSE disclosures of Canadian identity information. The objective of these annual reviews remains the same: to verify that CSE, in its disclosures of Canadian identity information, complied with the law, ministerial direction, and its policies and procedures, including assessing the extent to which it protected the privacy of Canadians.

DISCLOSURE OF CANADIAN IDENTITY INFORMATION

Information that may identify a Canadian is generally suppressed – that is, replaced by a generic term, such as "a named Canadian," as a measure to protect that Canadian's identity. CSE's Government of Canada clients and Second Party partners may request and receive this information if they have both the authority and operational justification to do so. The disclosure of Canadian identity information must be done in compliance with the *Privacy Act* and CSE's operational policy framework. To learn more about the authorities for and limitations on CSE activities, please visit the office's website.

This year, the Commissioner's office selected and examined a sample of 22 percent (236 requests) of the 1,067 requests from CSE's Government of Canada clients for disclosure of Canadian identity information contained in CSE reports. The review covered requests received by CSE from July 1, 2016, to June 30, 2017. All government institutions that made a request for Canadian identity information during that period were represented in the sample. In addition, the sample included all requests submitted by a particular Government of Canada client identified in the 2015–2016 review whose requests for Canadian identity information contained insufficient detail.

The office also examined all 62 requests from Second Party partners and the 7 requests made by two Government of Canada clients to share specified Canadian identity information with non-Five Eyes entities. CSE is responsible for conducting a mistreatment risk assessment when it releases the information; however, other Government of Canada institutions continue to be responsible for conducting a mistreatment risk assessment when the information is being released via their own channels. In disclosures involving non-Five Eyes recipients, CSE also includes a specific caveat to remind the requesting government client of its responsibility to conduct an assessment of the risks in sharing information with a foreign entity.

For this review, CSE was unable to provide copies of three original end-product reports as they existed at the time of the initial release of Canadian identity information because, subsequent to that release, they were cancelled or revised. The Commissioner's office understands that this practice is in compliance with CSE policy, as well as a measure to protect the privacy of Canadians. However, the result is that the office was unable to assess compliance in relation to these specific disclosures of Canadian identity information. The Commissioner's office has no reason to believe that these would not have been consistently handled as those the office did examine.

FINDINGS

The Commissioner was satisfied that:

- CSE disclosures of Canadian identity information complied with the law;
- the requesting Government of Canada client or Second Party partner had both the authority and operational justification for obtaining the information;
- CSE effectively applied the privacy protections contained in ministerial direction and in its operational policies and procedures; and
- CSE acted in accordance with the Cabinet framework for addressing risks in sharing information with foreign entities that could result in the mistreatment of an individual.

In January 2018, the Commissioner reported to the Minister of National Defence the results of his review of CSE disclosures of Canadian identity information for 2015–2016. This report included a recommendation that CSE strengthen its procedures so that it exercises a higher degree of diligence to ensure that all requests for release of Canadian identity information stipulate both the lawful authority under which the information is being requested, and a robust operational justification for the need to acquire that information, consistent with the requestor's mandate. The Commissioner expects to see evidence of CSE's action on that recommendation in his upcoming review of disclosures of Canadian identity information for 2017–2018. For this year's review, the Commissioner's office conducted a comparative analysis of disclosure requests from various Government of Canada clients, and identified instances where the legislative authority and/or operational justification in requests for the disclosure of Canadian identity information can be strengthened, not only for the Government of Canada client identified in the 2015–2016 review as providing insufficient details in requests, but for a few other Government of Canada clients as well.

On October 17, 2017, the ministerial direction entitled ***Avoiding Complicity in Mistreatment by Foreign Entities*** replaced the 2011 ministerial directive entitled ***Framework for Addressing Risks in Information Sharing with Foreign Entities***. While outside the period of this review, implementation of this new ministerial direction

will be monitored during next year's review of disclosures of Canadian identity information.

Since the 2015–2016 review, CSE made neither policy amendments nor technical changes to its process for the disclosure of Canadian identity information. Although CSE advised during past reviews that it was assessing options for automating the process for disclosures of Canadian identity information to Second Parties, no such technical changes occurred during the period under review.

CONCLUSION

The review did not result in any recommendations.

One matter arose that is being examined separately so that the 2016–2017 review could be reported to the Minister by the end of the fiscal year. In approving a Government of Canada client request for Canadian identity information, concerns were raised about a CSE metadata analysis activity. This separate review was ongoing as of March 31, 2018.

The office will continue to conduct annual reviews of CSE disclosures of Canadian identity information to clients and partners to verify that CSE complies with the law and protects Canadians' privacy.

5. Annual Review of CSE Cyber Defence Activities Conducted Under Ministerial Authorization, 2016–2017

BACKGROUND

CSE conducts cyber defence activities under the authority of paragraph 273.64(1)(b) of the ***National Defence Act*** – part (b) of its mandate. This part of the mandate authorizes CSE to help protect electronic information and information infrastructures of importance to the Government of Canada, more familiarly known as information technology (IT) security. Activities conducted pursuant to part (b) of CSE's mandate shall not be directed at Canadians anywhere or at any person in Canada, and shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information (paragraphs 273.64(2)(a) and (b) of the ***National Defence Act***).

Cyber defence activities involve both detecting and protecting against sophisticated cyber threats. On receiving a written request from a Government of Canada institution to conduct cyber defence activities, CSE may deploy measures to collect and analyze data from that client's system or network. Because cyber defence activities

risk the interception of private communications, CSE must conduct these activities under the authority of a ministerial authorization. Subsection 273.65(3) of the ***National Defence Act*** permits the Minister to authorize CSE in writing – for the sole purpose of protecting the computer systems or networks of the Government of Canada from cyber threats – to intercept private communications in relation to an activity or class of activities specified in a ministerial authorization. In cyber defence activities, data intercepted by CSE, including any private communications, may be used or retained only if it is relevant and essential to identify, isolate or prevent harm to Government of Canada computer systems or networks.

MINISTERIAL AUTHORIZATIONS

Ministerial authorizations shield CSE from the prohibition respecting the interception of private communications found in Part VI of the *Criminal Code*. A ministerial authorization is a written document by which the Minister of National Defence authorizes CSE to engage in an activity or class of activities that risks the interception of private communications. Authorizations cannot be in effect for a period of more than one year. To learn more about the authorities for and limitations on CSE activities, please visit the office's website.

This review covered the ministerial authorization for cyber defence activities in effect from July 1, 2016, to June 30, 2017. The purpose of the review was to assess whether CSE's cyber defence activities complied with the law and to assess the extent to which CSE protected the privacy of Canadians. In conducting this review, the Commissioner's office examined CSE's 2014–2015, 2015–2016 and 2016–2017 ministerial authorization request memoranda to the Minister of National Defence, the associated ministerial authorizations, as well as the 2016–2017 CSE Year-End Ministerial Authorization Report to the Minister. The office received on-site briefings, conducted interviews, reviewed CSE databases and systems, and examined various types of reports, both internal and external. The office selected for examination a 36-percent sample of the cyber incidents, which included private communications.

FINDINGS AND RECOMMENDATION

The Commissioner found that the 2016–2017 cyber defence ministerial authorization met the conditions for authorization set out in the ***National Defence Act***. CSE made no significant changes to the ministerial authorization or conduct of cyber defence activities that affected the risk of non-compliance with the law or to privacy. During this review period, there were no significant amendments to policy instruments governing cyber defence activities conducted under ministerial

authorization. There was no evidence that CSE conducted cyber defence activities contrary to legislative, ministerial or policy requirements. Based on an examination of recognized private communications that CSE intercepted, the Commissioner found that CSE did not direct cyber defence activities at Canadians or any person in Canada. The majority of private communications examined related to malicious traffic or activity and suspicious anomalies for cyber threat detection. The private communications retained and used in reports were essential to identify, isolate or prevent harm to Government of Canada computer systems or networks.

Definition of Solicitor-Client Communications

The Commissioner made one recommendation, based on a change in terminology used by CSE in the cyber defence ministerial authorization regarding solicitor-client communications. The ministerial authorization specifies the measures to be taken when a CSE analyst recognizes a communication between a client and a "Canadian solicitor." The Commissioner's office sought clarification from CSE on the addition of the qualifier Canadian, which was not explicitly mentioned in previous ministerial authorizations. CSE advised that the Canadian qualifier was not new and had been included in the ministerial authorization for clarity. The Commissioner, however, found that the inclusion of this qualifier created ambiguity. Further, specifying that a solicitor-client communication involves a Canadian solicitor meant that the ministerial authorization was inconsistent with CSE policy and CSE practice.

Based on the definition of Canadian found in the ***National Defence Act***, the term Canadian connotes citizenship – referring to a Canadian citizen, a permanent resident or a body corporate incorporated in Canada – regardless of location. The Commissioner expects ministerial authorizations to use terms as they are defined in the ***National Defence Act***. However, CSE advised that, in practice, it relies on the definition of solicitor-client communication found in its overarching privacy policy, which does not use the term Canadian, nor refer to citizenship or geographic location. Rather, the definition is based on whether the person is authorized to practise as a solicitor in Canada. Therefore, when solicitor-client communications are intercepted, CSE must be mindful not only of whether a solicitor is "Canadian," but also where the solicitor is located (within or outside of Canada) and whether the solicitor is authorized to practise law in Canada.

In reviewing CSE's overarching privacy policy instrument, the Commissioner's office noted that the definition of a solicitor-client communication only addresses the handling of these communications under CSE's foreign signals intelligence and assistance mandates – it does not explicitly apply to CSE's IT security mandate. Another policy specific to CSE's IT security mandate does include a section on solicitor-client communications; however, it does not use the term Canadian solicitor, nor does it define a solicitor-client communication. The instructions

concerning the handling of a solicitor-client communication in this policy also lack procedural clarity. CSE has advised that it has since modified this policy. The Commissioner's office will assess these changes as part of next year's review.

The Commissioner believes there are inconsistencies in the definition of solicitor-client communication as found in the ministerial authorizations for cyber defence activities and foreign signals intelligence, as applied in CSE practices, and as found in the IT security policy. Therefore, the Commissioner **recommended** that CSE clarify the language in its ministerial authorizations to accurately reflect the legal protection recognized and afforded to solicitor-client communications in Canadian law, and to ensure consistency with language in its policies and practices in both IT security and foreign signals intelligence activities. The Commissioner will monitor developments concerning this matter.

Cyber Defence Private Communications

The Commissioner's office selected and examined a sample of cyber defence data, which included private communications intercepted by CSE in 2016–2017. Specifically, the office examined a 36-percent sample of cyber incidents and a randomly selected number of incidents where the private communication count was indicated to be zero. For the period under review, CSE did not intercept any solicitor-client communications. As in previous years, the majority of the private communications intercepted consisted of unsolicited e-mails from a cyber threat actor to a Government of Canada employee.

CYBER INCIDENT
A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of electronic devices and communications networks of importance to the Government of Canada. A cyber incident may involve one or more cyber events and one or more private communications.

During the period of this review, the Commissioner noted an increase in the number of private communications used or retained. Last year, CSE upgraded its repository for used and retained cyber defence data and the system for tracking records related to private communications that CSE collects under its IT security mandate. CSE confirmed the increase in the number of private communications is primarily attributed to this upgrade, which has improved CSE's capacity to discover and promptly retain relevant cyber threat information, including private communications. Intercepted data, including any private communications, may be retained or used by CSE only if it is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks. Automation has

increased the consistency of CSE's private communication counting methods in that private communications are automatically counted at the time of retention.

In reviewing private communications at CSE, the Commissioner's office noted the existence of what CSE refers to as "incidentally collected PCs." These are private communications that are **not** essential to the protection of Government of Canada systems that are captured in files during network interception. Although CSE does not use these incidentally collected private communications, CSE retains the files for 12 months because the files also contain private communications that are essential to the protection of Government of Canada systems. The files are kept in accordance with the authorized ministerial authorization period, after which they are automatically deleted. The Commissioner's office accepts CSE's explanation that this is a technology limitation and confirmed that this retention period is being respected for the current review period. The Commissioner will continue to monitor CSE handling of incidentally collected private communications in its annual reviews.

During the review of the sample, and guided in part by a CSE quarterly compliance monitoring activity, the Commissioner's office noted a cyber incident record solely for internal use that included unsuppressed Canadian identity information. This internal document that CSE uses for cyber defence analysis is accessible to all CSE cyber defence analysts. While it was clear that the Canadian identity information contained in the internal record was relevant to the cyber incident, the Commissioner's office questioned whether it was necessary for CSE to include detailed personal information belonging to the victim, rather than just summarizing the types of information that were found in the cyber incident. The Commissioner's office noted that while access controls are in place and a caveat is included with the internal record about its use and retention, in future this caveat could be further strengthened by explicitly stating a requirement for privacy protection where unsuppressed Canadian identity information is included. The Commissioner's office has encouraged CSE to consider privacy implications for both its reports and its internal records, and will continue to monitor the inclusion of Canadian identity information in internal records.

As noted, the majority of the private communications that CSE counted as retained or used in 2016–2017 consisted of unsolicited e-mails sent from a cyber threat actor to a Government of Canada employee. They contained nothing more than malicious code and/or an element of social engineering – that is, there was no exchange of any personal or other consequential information between the cyber threat actor and the employee. Contrary to the Commissioner's views, CSE counts these types of communications as private communications.

CYBER DEFENCE PRIVATE COMMUNICATIONS: WHAT THE COMMISSIONER SAYS

"A communication containing nothing more than malicious code or an element of social engineering sent to a computer system in order to compromise it is **not** a private communication as defined by the *Criminal Code*."

Source: CSE Commissioner Annual Report 2015-2016

However, CSE indicated it continued to work with the Department of Justice to clarify the definition of a private communication in an IT security context, aiming to make it consistent with the Commissioner's 2015–2016 legal interpretation. The Commissioner's office was advised that CSE is considering a change to its procedures for counting cyber defence private communications, the end result of which would be to eliminate those that are computer-generated (i.e., spam) from the official count. It is positive that CSE is reconsidering its interpretation of the definition of a private communication as defined by the *Criminal Code*.

Last year, the Commissioner's office noted an expansion of the situations where certain Canadian identity information associated with compromised or targeted infrastructure may be disclosed, unsuppressed, to select Government of Canada institutions, private sector entities and Second Party partners. The Commissioner noted that CSE should work with its Second Party partners to finalize an information-sharing agreement for cyber security. The Commissioner is pleased to confirm that CSE has finalized a policy statement for the sharing among the Five Eyes of identity information in relation to cyber defence activities. The policy stipulates the types of identities for dissemination, the conditions under which this may occur and the caveats that must be respected. The Commissioner found the policy to be an acceptable baseline for the sharing of such information, particularly given the condition that the dissemination must be necessary to the analysis and mitigation of the cyber security threat.

The Commissioner also committed to follow up on CSE's pilot to use a malware analysis system deployed under its existing authorities. The Commissioner's office has confirmed that data retention and access for this system, now in production, is consistent with existing CSE policies and subject to quarterly compliance monitoring.

CONCLUSION

CSE has taken steps to address the Commissioner's recommendation from the 2015–2016 cyber defence ministerial authorization review that CSE promulgate guidance on the consistent annotation and counting of what constitutes a cyber defence private communication. CSE has implemented new guidance and training,

as well as upgraded its repository for used and retained cyber defence data, in order to automate the identification of potential private communications and standardize the counting of cyber defence private communications. The Commissioner is pleased to confirm that, with these steps, CSE has fulfilled this recommendation.

CSE made no significant changes to the conduct of cyber defence activities or any changes that affected the risk of non-compliance with the law or to privacy. All private communications that were recognized by CSE were intercepted unintentionally and treated in accordance with CSE policies and procedures – nothing suggested that CSE directed any of its cyber defence activities at Canadians or at any person in Canada. The private communications that were used and retained by CSE were essential to identify, isolate or prevent harm to Government of Canada computer systems or networks, as required by the *National Defence Act* for part (b) of CSE's mandate. Those private communications that were non-essential were not retained beyond the retention and disposition periods prescribed by CSE policy.

The Commissioner will continue to conduct annual reviews of cyber defence ministerial authorizations and private communications to verify that such activities are authorized, that CSE does not target Canadians and that CSE protects the privacy of Canadians.

6. Annual Combined Review of CSE Foreign Signals Intelligence Ministerial Authorizations, 2016–2017 and 2017–2018, and a One-End Canadian Communications Spot Check

BACKGROUND

This summary combines the findings of two reviews.

- **The annual foreign signals intelligence ministerial authorizations review:** The review of foreign signals intelligence ministerial authorizations was executed under the *National Defence Act*, which requires the Commissioner to review CSE activities under ministerial authorizations to ensure they are authorized, and to report annually to the Minister on the results of the review. The office also reviewed the status, at the end of the ministerial authorization period, of private communications retained or used by CSE that were intercepted under these ministerial authorizations.

- **A spot check review of one-end Canadian communications:** The spot check review was conducted under the Commissioner's main mandate to review CSE's activities to ensure that they are in compliance with the law. The review examined one-end Canadian communications retained, used or deleted by CSE during a two-month period in 2017. They include those intercepted by Second Party partners and transmitted to CSE.

PRIVATE COMMUNICATIONS AND ONE-END CANADIAN COMMUNICATIONS

Canadian means a Canadian citizen, a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act*, or a body corporate incorporated and continued under the laws of Canada or a province.

Private communication is defined in section 183 of the *Criminal Code* as "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it."

One-end Canadian communication means a communication where one of the communicants is physically located in Canada (i.e., a private communication) or one communicant is a Canadian physically located outside Canada. Such a communication may be acquired either by CSE or by Five Eyes partners and transmitted to CSE.

CSE conducts foreign signals intelligence collection activities under the authority of paragraph 273.64(1)(a) of the *National Defence Act* – part (a) of CSE's mandate – to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence in accordance with Government of Canada intelligence priorities. These activities must not be directed at Canadians anywhere or at any person in Canada, and must include measures to protect the privacy of Canadians in the use, and retention of, intercepted information (paragraphs 273.64(2)(a) and (b) of the *National Defence Act*).

Subsection 273.65(1) of the *National Defence Act* permits the Minister to authorize CSE in writing, for the sole purpose of obtaining foreign intelligence, to intercept private communications in relation to an activity or class of activities specified in the ministerial authorization. Since foreign signals intelligence activities risk the

unintentional interception of private communications, CSE must conduct these activities under the authority of a ministerial authorization. CSE can retain or use an intercepted private communication only if it is deemed essential to international affairs, defence or security. All collected information used in a foreign intelligence report is retained indefinitely by CSE.

INCIDENTAL AND UNINTENTIONAL

In describing the interception of a private communication under a ministerial authorization, CSE qualifies the interception using the term "incidental," whereas the Commissioner's office uses the term "unintentional." Why and what is the difference?

The "incidental" interception of a private communication occurs when CSE intercepts communications between a foreign entity located outside Canada and a person in Canada.

"Unintentional" is a legal description of the "incidental" interception of a private communication made by CSE in a technical or operational context. It is "unintentional" in a legal perspective because the interception was not done with the aim of targeting a Canadian or a person in Canada, but rather as a by-product or a subordinate part of the targeting of a foreign entity located outside of Canada.

During 2017–2018, CSE conducted foreign signals intelligence collection activities under ministerial authorizations – three of which were in effect July 1, 2016, to June 30, 2017, and three that came into effect on July 1, 2017, and expire on June 30, 2018. The office reviewed all these ministerial authorizations.

The objectives of the review were: to ensure the ministerial authorizations were authorized, that is, that the conditions for authorization set out in subsection 273.65(2) of the ***National Defence Act*** were satisfied; to identify any significant changes – for the years under review, compared with previous years – to the ministerial authorization documents themselves and to CSE activities or class of activities described in the ministerial authorizations; and to assess the impact, if any, of the changes on the risk of non-compliance with the law and on the risk to privacy.

The office examined the status, at the end of the 2016–2017 ministerial authorization period, of the recognized private communications that CSE had acquired, retained or used in carrying out its foreign signals intelligence activities. The office verified CSE's compliance with the law and with all applicable authorizations, ministerial directives and policies, and assessed the extent to which CSE protected the privacy of Canadians. In addition, the Commissioner's office

conducted a spot check review – with no notice given to CSE – of all one-end Canadian communications (which include private communications) used or retained by CSE during a two-month period in 2017.

For both the private communications acquired under ministerial authorization and the one-end Canadian communications that were part of the spot check review, the office examined all foreign intelligence reports produced by CSE that were based in whole, or in part, on these communications. The office also received briefings on all of these communications that were retained, viewed a sample of them directly, and interviewed the foreign intelligence analysts and supervisors concerned – who were working on government intelligence priorities – about their justification for retaining the communications.

FINDINGS AND RECOMMENDATIONS

The Commissioner found that the 2016–2017 and 2017–2018 foreign signals intelligence ministerial authorizations met the conditions for authorization set out in the ***National Defence Act***, namely that:

- the interception was directed at foreign entities located outside Canada;
- the information could not have been reasonably obtained by other means;
- the expected foreign intelligence value of the information justified the interception; and
- satisfactory measures were in place to protect the privacy of Canadians and that private communications were used or retained only if they were essential to international affairs, defence or security.

There were no major changes to the 2016–2017 and 2017–2018 ministerial authorizations and associated request memoranda to the Minister. However, it was determined that the request memorandum associated with one of the ministerial authorizations contained less detail than in previous years. In 2017–2018, CSE revised the request memorandum for one of the ministerial authorizations to consistently describe CSE sampling and selection activities. While the quest for consistency is positive, the Commissioner found that some detail regarding process and technical explanation was lost in the effort and resulted in a memorandum that may not be as informative as possible to the Minister when he is making a decision. Therefore, the Commissioner **recommended** that CSE ensure that future ministerial authorization request memoranda contain comprehensive information to describe and document contemplated CSE foreign signals intelligence activities in a thorough manner, to better support the Minister when making a decision.

PROTECTION OF CANADIANS' PRIVACY

CSE is prohibited from directing its foreign signals intelligence and cyber defence activities at Canadians anywhere in the world or at any person in Canada. The foreign focus of CSE's work means that, unlike Canada's other security and intelligence agencies, CSE has limited interaction with Canadians. When CSE does incidentally acquire information relating to a Canadian, it is required by law to take measures to protect the privacy of the Canadian. The Commissioner's review of CSE activities includes verifying that CSE does not target Canadians and that CSE effectively applies satisfactory measures to protect the privacy of Canadians in all its operational activities.

In 2016–2017, the number of recognized private communications unintentionally intercepted continued to increase substantially. The increase in the number of recognized private communications remains a consequence of the technical characteristics of certain communications technologies, and CSE's legal obligation to count private communications in a certain manner. Despite the increase in intercepted private communications, the number of private communications that were used or retained decreased by approximately 70%, from 3,348 to 954, at the end of the 2016–2017 ministerial authorization period.

CSE used 261 of these 954 private communications in 14 foreign intelligence reports and subsequently deleted the remaining private communications.

During the spot check review, the office also reviewed all the one-end Canadian communications that were unintentionally acquired during a specified time frame and subsequently recognized as such. These included both communications marked for retention and those marked for deletion by CSE as not being essential to international affairs, defence or security.

The office confirmed that those one-end Canadian communications that were not found to be essential were deleted from CSE systems.

Based on the information reviewed and the interviews conducted, the Commissioner found that CSE complied with the law and protected the privacy of Canadians. Specifically:

- CSE did not direct its foreign signals intelligence activities at Canadians or persons in Canada;
- one-end Canadian communications recognized by CSE were intercepted unintentionally;
- one-end Canadian communications used and retained by CSE were essential to international affairs, defence or security, as required by the ***National Defence Act***;

- CSE deleted non-essential one-end Canadian communications; and
- CSE conducted its foreign signals intelligence activities in accordance with applicable ministerial authorizations and directives, and treated one-end Canadian communications in accordance with its policies and procedures – CSE did not retain private communications beyond the retention and disposition periods prescribed by its policy.

Definition of Solicitor-Client Communications

The Commissioner's office noted a change in terminology used by CSE in the three ministerial authorizations regarding solicitor-client communications. The authorizations specify the measures to be taken when a CSE analyst recognizes a communication between a client and a "Canadian solicitor." The Commissioner's office sought clarification from CSE on the addition of the qualifier Canadian, which was not explicitly mentioned in previous ministerial authorizations. CSE responded that this qualifier was not new and was included in the ministerial authorizations for clarity. The Commissioner is of the view that the inclusion of this qualifier creates ambiguity.

The term Canadian connotes citizenship, regardless of the location of the solicitor. The definition of Canadian, as found in the ***National Defence Act***, means a Canadian citizen, a permanent resident or a body corporate incorporated in Canada. The Commissioner expects ministerial authorizations to use terms as they are defined in the ***National Defence Act***. In practice, however, CSE relies on the definition of solicitor-client communication found in its overarching privacy policy, which does not use the term Canadian, nor refer to citizenship or geographic location. Rather, the definition is based on whether the person is authorized to practise as a solicitor in Canada.

This issue applies to both the foreign signals intelligence and the information technology security ministerial authorizations. Therefore, **the Commissioner made the same recommendation** as he did in his annual review of CSE's cyber defence activities conducted under ministerial authorization in effect in 2016–2017, that CSE clarify the language in the ministerial authorizations to accurately reflect the legal protection recognized and afforded to solicitor-client communications in Canadian law, and ensure consistency with language in policy and with practice, in both CSE's information technology security and foreign signals intelligence activities.

Evolving Legal Landscape

Recently, the Supreme Court of Canada considered two cases (***R v Marakah***, 2017 SCC 59 and ***R v Jones***, 2017 SCC 60) that addressed the concepts of "intercept" and "search" in the context of evolving technology. These cases were of interest as they could have impacted the handling of one-end Canadian communications

acquired under one of CSE's foreign signals intelligence collection programs. Ultimately, the decisions rendered did not affect CSE's operations; however, the evolving legal landscape may influence guidelines on how certain one-end Canadian communications are handled in the future. The Commissioner will monitor any legal developments and their resulting effect on CSE activities.

CONCLUSION

Since the last review of the ministerial authorizations for foreign signals intelligence activities, CSE has addressed two recommendations introduced in last year's annual report: one that was issued in the foreign signals intelligence ministerial authorization review, and the other issued in the spot check review. The first recommendation suggested that because of the technical characteristics of certain communications technology, CSE reporting to the Minister on private communications should include additional information to better describe the private communications and explain the extent of privacy invasion; the current manner in which CSE counts private communications provides a distorted view of the number of Canadians or persons in Canada that are involved in (i.e., are the other end of) CSE interceptions to obtain foreign intelligence under ministerial authorizations. In its year-end ministerial authorization report to the Minister for 2016–2017, the Commissioner was satisfied that CSE provided the additional information to the Minister to explain the reason for the substantial increase in the number of recognized private communications.

The second recommendation suggested that whenever contemplating the use and/or retention of an intercepted solicitor-client privileged communication, CSE should always seek and obtain written legal advice from Justice Canada concerning the privileged nature of the communication and on whether the retention and/or use of the solicitor-client communication would be in conformity with the laws of Canada. CSE modified its policy to describe what is expected of CSE employees when handling solicitor-client communications collected under CSE's foreign signals intelligence mandate, which includes seeking legal advice and retaining records of decisions made and the legal advice obtained.

The Commissioner's office will continue to conduct annual reviews of foreign signals intelligence ministerial authorizations, as well as reviews of CSE's foreign signals intelligence collection activities conducted pursuant to the ministerial authorizations. The office will also conduct in-depth spot check reviews of one-end Canadian communications acquired and recognized by CSE, whether collected by CSE or a Second Party partner. In addition, the Commissioner's office intends to examine, in a follow-up review, how different CSE programs may complement and impact each other.

Finally, the Commissioner will monitor CSE actions to address matters identified in this report.

7. Annual Review of Privacy Incidents and Minor Procedural Errors Files

BACKGROUND

CSE reports and documents any incidents that are associated with its operational activities, or those of its Second Party partners, where the privacy of a Canadian may have been put at risk contrary to CSE operational policy or procedures on protecting the privacy of Canadians or any person in Canada.

Such incidents, along with corrective actions taken, are recorded in one of three files, depending on where the incident occurred and its potential to cause harm. These are CSE's Privacy Incidents File (PIF), the Second Party Incidents File (SPIF) and the Minor Procedural Errors File (MPEF).

The PIF is a record of incidents attributable to CSE involving information about a Canadian or any person in Canada that was handled in a manner counter to CSE privacy policy and exposed to external parties who ought not to have received it. This type of mishandling is labelled a "privacy incident." The SPIF is a record of privacy incidents that are attributable to Second Party partners. These incidents may be identified by the partners themselves, or by CSE. The MPEF is a record of instances where CSE improperly handled information about a Canadian but the information was contained within CSE and not exposed to external parties.

The office's annual review of the PIF, SPIF and MPEF focuses on incidents not examined in detail in the course of other reviews. The review is an opportunity to identify trends or systemic weaknesses that might suggest a need for corrective action, changes to CSE's procedures or policies, or an in-depth review of a specific incident or activity. For example, the office could challenge whether an incident constituted an operational "material privacy breach," which government-wide policy defines as a breach that involves sensitive personal information and could reasonably be expected to cause serious injury or harm to the individual and/or involves a large number of affected individuals.

Besides reviewing the procedural errors, incidents and subsequent actions taken by CSE to correct the incidents or mitigate the consequences, the objectives of the review were: to assess whether incidents constituted operational material privacy breaches; to determine if any incidents raise questions about compliance with the law or the protection of the privacy of Canadians; and to evaluate CSE's policy compliance validation framework and monitoring activities in this context. The review period was from July 1, 2016, to June 30, 2017.

The office examined all 81 privacy incidents in the PIF (48) and SPIF (33) and subsequent corrective actions taken by CSE to address them. The office also

examined the 10 minor procedural errors documented by CSE during the review period.

FINDINGS

Most of the privacy incidents in both the PIF and SPIF involved the inadvertent sharing or inclusion in a report of Canadian identity information without suppressing the information in accordance with CSE policy, as well as the unintentional targeting or database searches for information relating to individuals not previously known to be Canadian or persons in Canada. In all instances, the reports were cancelled or corrected with the identities properly suppressed, or CSE deleted any associated intercepted communications or reporting.

CANADIAN IDENTITY INFORMATION

Canadian identity information refers to information that may be used to identify a Canadian person, organization or corporation, in the context of personal or business information. Canadian identity information includes, but is not limited to, names, phone numbers, e-mail addresses, Internet protocol addresses and passport numbers. When CSE includes Canadian identity information in a report, this information must be suppressed and replaced with a generic term, such as "a named Canadian," as a measure to protect that Canadian's identity.

Two incidents involved gaps in awareness or understanding of CSE's Canadian privacy protection policies by groups external to CSE: one group belonged to a Second Party and the other to a Canadian partner. In both cases, the groups concerned received remedial policy awareness materials from their organizations.

For the third year in a row, the PIF included an incident involving a report containing information about a Canadian or a person in Canada that a Five Eyes partner provided to the Canadian Security Intelligence Service, via CSE, that should have had a limited internal distribution but was shared within CSE. However, this report was distributed in an urgent, threat-to-life situation. The Commissioner was satisfied that, although the employee's actions were contrary to CSE policy, CSE's response was appropriate given the circumstances. The office was later informed that corrective policy measures have been formalized. This incident will be examined in depth in the office's review of CSE's assistance to the Canadian Security Intelligence Service regarding this type of activity, which will start in the next fiscal year.

A PIF entry concerned a malfunctioning collection tool that allowed Canadian identity information to be pulled into CSE repositories over approximately

10 days. The tool was corrected and the data that was collected inadvertently was purged from CSE's systems.

The Commissioner agreed with CSE that all of the MPEF entries were minor and did not constitute privacy incidents. These procedural errors included, for example: unopened files that may have contained Canadian identity information that were kept beyond the allowed retention period; a list that controlled access to certain types of information technically malfunctioned and temporarily did not disable access to persons whose credentials were no longer valid; Canadian identity information was temporarily visible on an internal communication tool; and another malfunctioning collection system that, for a period, risked collecting two-end Canadian information but did not do so. The privacy impact of such incidents is considered less severe since they were contained internally and addressed prior to the information being accessed by anyone outside CSE.

Based on a review of the three files, CSE's answers to questions and the examination of associated CSE records, the Commissioner found that CSE took appropriate corrective action in all instances, including, where feasible, instituting measures to preclude similar occurrences in the future.

According to government-wide policy, it is a department's or agency's responsibility to identify material privacy breaches. CSE did not identify any operational material privacy breaches as having occurred during the period under review. The Commissioner agreed that the incidents listed in the PIF and SPIF for this review period did not constitute material privacy breaches.

CONCLUSION

This review did not identify any material privacy breaches, systemic deficiencies or issues that require follow-up review that was not already planned. CSE reported that it did not know of any adverse impact on the Canadian subjects of any of the privacy incidents.

The Commissioner was satisfied that CSE responded appropriately to privacy incidents and minor procedural errors identified during the review period.

The recording and reporting of privacy incidents and minor procedural errors continues to be an effective means for CSE to promote compliance with legal and ministerial requirements, and with operational policies and procedures, as well as to enhance the protection of the privacy of Canadians. The improvements made in relation to this reporting and to associated file structures should further strengthen privacy protections.

The Commissioner made no recommendations. However, he encouraged CSE to ensure consistency of use and meaning regarding the terms used in reporting between its foreign signals intelligence and information technology security activities.

COMPLAINTS ABOUT CSE ACTIVITIES

In 2017–2018, the office was contacted by a number of individuals who were seeking information or expressing concern about CSE activities. However, the inquiries were assessed as outside of the Commissioner's mandate, not related to CSE operational activities or without merit. There were no complaints about CSE activities that warranted investigation.

DUTY UNDER THE *SECURITY OF INFORMATION ACT*

The Commissioner has a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to defend the release of special operational information – on the grounds that is in the public interest. No such matters were reported to the Commissioner in 2017–2018.

ACTIVITIES OF THE OFFICE

LEGISLATIVE CHANGES

The Commissioner and his officials devoted considerable effort throughout the year to examining two bills before Parliament that aim to strengthen the accountability of federal government departments and agencies involved in national security activities.

Both bills proposed important changes to Canada's intelligence and security landscape. Commissioner Plouffe met with the ministers of National Defence and Public Safety, the National Security and Intelligence Advisor to the Prime Minister, and the Chief of CSE. The Commissioner's staff held numerous meetings with officials from CSE, the Canadian Security Intelligence Service (CSIS), Public Safety Canada, the Privy Council Office and the Security Intelligence Review Committee (SIRC). These fruitful exchanges informed everyone's understanding and promoted further exploration of the ideas put forward in the bills.

BILL C-22

As part of the restructuring of the national security accountability framework, Bill C-22, An Act to establish the National Security and Intelligence Committee of Parliamentarians (NSICOP), was tabled in the House of Commons in 2016. In his appearance before the Senate Standing Committee on National Security and Defence on June 12, 2017, Commissioner Plouffe articulated his vision for a productive working relationship with the NSICOP to help ensure the most effective and efficient use of respective resources. He also pointed out factors to consider in avoiding duplication of effort between the NSICOP and the review bodies.

The bill received Royal Assent on June 22, 2017; committee members were appointed in the fall of 2017 and the executive director of the NSICOP secretariat was appointed in January 2018.

BILL C-59

The same week that Bill C-22 was passed, the government tabled another substantial bill, C-59, An Act respecting national security matters. The bill was sent to the House of Commons Standing Committee on Public Safety and National Security (SECU) before second reading, rather than the usual practice of sending it after second reading. The government chose this process to allow, as Minister Goodale stated, new ideas and alternative suggestions to be presented before second reading.

The 10-part bill is complex and will transfer the office's review function to the proposed National Security and Intelligence Review Agency. It also provides for the CSE Commissioner to become the Intelligence Commissioner, who will be involved in the decision-making process for certain activities proposed by CSE and CSIS before the activities can be undertaken.

Commissioner Plouffe appeared before SECU, along with the office's Executive Director and Special Legal Advisor, on January 30, 2018. The Commissioner highlighted several of the proposals he had made in the written submission to SECU, including suggestions to match the new powers for CSE with a broader role for the Intelligence Commissioner.

In the latter part of the year, CSE and the Department of Justice organized information sessions to help other departments and agencies involved in national security activities better understand the implications of Bill C-59 for their operations. The Commissioner's office was pleased to participate and explain what review is, what it isn't and how it is conducted. Preparing these departments and agencies for how they may be affected helps both to ensure that expectations are realistic and to dispel concerns.

OUTREACH, LEARNING AND NETWORKING

The Commissioner and his office represent the public interest in the accountability of CSE because CSE must operate largely in secret. The office's outreach, networking and learning activities contribute to the transparency the Commissioner strives for and strengthen the office's ability to deliver on the Commissioner's mandate.

In August, the Executive Director spoke to a summer graduate course at the University of Ottawa about review past and future, describing the Commissioner's current role and how Bill C-59 could restructure the national security accountability framework.

In October, the Canadian Forces Communications and Electronics Association organized a Cyber Ops Symposium in Kingston, Ontario, that brought government and industry practitioners together with academic specialists. The Executive Director participated in a panel dealing with the proposed legislation for oversight of national security activities and its impact on cyber operations.

Two legal advisors from the Commissioner's office spoke in March to graduate students of the University of Sherbrooke about the Commissioner's authorities and activities. Representatives of SIRC and the NSICOP secretariat also spoke.

The Executive Director attended the 19th Annual Privacy and Security Conference in Victoria, British Columbia, in February 2018. This eminent event, at which the Executive Director has spoken twice before, brings together government, industry and academia to hear about and discuss the latest developments in Canada and internationally in technology, security and privacy.

Throughout the year, office staff attended conferences dealing with international affairs, information technology security, national security, privacy and cyber security. These conferences were held by such organizations as the Smart Cybersecurity Network, the Canadian Association of Security and Intelligence Studies, and various academic institutions.

Through training, office staff maintained and enhanced professional standards in various fields, including the law, access to information and privacy, and communications security.

In addition, a day and a half workshop on review – an initiative the Commissioner's office launched eight years ago – was held in February. Designed to fill a training gap for reviewers of intelligence and security agencies, particularly for personnel new to the review function, the most recent workshop was delivered to employees from the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police, SIRC, and the NSICOP secretariat, in addition to employees of the Commissioner's office.

The office also continued to deliver presentations about its work to new CSE employees as part of CSE's foundational learning curriculum. Several office employees attended courses at CSE, grounding them in the same information CSE employees receive.

MEETINGS WITH OTHER REVIEW BODIES

Last year, the Commissioner reported on meetings he and his colleague, the Chair of SIRC, had in Washington, D.C., in 2016 with their counterparts from the United States, the United Kingdom, Australia and New Zealand. Such meetings are essential in an environment where our respective countries are seeing significant legislative changes that affect accountability structures and create new authorities for security and intelligence agencies.

Out of the Washington meeting came an agreement to establish the Five Eyes Intelligence Oversight and Review Council. The first in-person meeting of this Council was held over two days in October, co-hosted by the CSE Commissioner and the Chair of SIRC. All participants agreed that the discussions were very productive and will help strengthen the overall accountability of security and intelligence activities in our respective countries. The Council established that an in-person meeting will be held annually, with video-teleconferences between these meetings.

One impetus for creating the Council was the demise of the International Intelligence Review Agencies Conference. While the Council allows the Commissioner to enhance closer ties with his Five Eyes counterparts, the Commissioner also strives to maintain contact with a number of his other international counterparts that had participated in the conference.

Other meetings in Canada with foreign officials included the Investigatory Powers Commissioner from the United Kingdom in October and the Netherlands National Coordinator for Security and Counter-Terrorism in March. The office also participated in a meeting focused on intelligence oversight, organized by SIRC, which was held with the Parliamentary Committee for the Security of the Italian Republic in November.

WORK PLAN – REVIEWS UNDER WAY AND PLANNED

The Commissioner uses a risk-based and preventive approach to reviews, setting priorities of what to review where risk is assessed as greatest for potential non-compliance with the law or as a potential threat to the privacy of Canadians. A three-year work plan is updated twice a year. Developing the work plan draws on many sources, including: regular briefings from CSE on new activities and changes to existing activities; the classified annual report to the Minister from the Chief of CSE on priorities and legal, policy, operational and management issues of significance; and issues raised in past or ongoing reviews. To learn more about the Commissioner's risk-based and preventive approach to reviews, please visit the office's website.

Once Bill C-59 is in effect, the Commissioner's office's ongoing reviews will be transferred to the National Security and Intelligence Review Agency for completion. However, the office expects that the four reviews that are carried over from 2017–2018 will be completed in 2018–2019. These are: a review of a particular method of collecting foreign signals intelligence conducted under a ministerial authorization and a ministerial directive; a review of CSE targeting activities; a review of CSE assistance to the Canadian Security Intelligence Service (CSIS) under part (c) of CSE's mandate and sections 12 and 21 of the *CSIS Act* (formerly, this type of CSE assistance was executed under what was called Domestic Intercept of Foreign Telecommunications and Search warrants); and a separate review that derived from the concluded 2016–2017 review of CSE disclosures of Canadian identity information.

A follow-up review will also be conducted on CSE support to CSIS under part (c) of CSE's mandate regarding a certain type of reporting involving Canadians.

The Commissioner will continue to conduct annual reviews of:

- foreign signals intelligence and cyber defence ministerial authorizations, including spot check reviews of one-end Canadian communications acquired and recognized by CSE;
- CSE disclosures of Canadian identity information; and
- privacy incidents and procedural errors identified by CSE and the measures subsequently taken by CSE to address them.

ANNEX A: BIOGRAPHY OF THE HONOURABLE JEAN-PIERRE PLOUFFE, CD

The Honourable Jean-Pierre Plouffe was appointed Commissioner of the Communications Security Establishment effective October 18, 2013, for a period of three years. On October 18, 2016, he was re-appointed for a two-year term.

Mr. Plouffe was born on January 15, 1943, in Ottawa, Ontario. He obtained his law degree, as well as a master's degree in public law (constitutional and international law), from the University of Ottawa. He was called to the Quebec Bar in 1967.

Mr. Plouffe began his career at the office of the Judge Advocate General of the Canadian Armed Forces. He retired from the Regular Force as a Lieutenant-Colonel in 1976, but remained in the Reserve Force until 1996. He worked in private practice with the law firm of Séguin, Ouellette, Plouffe et associés, in Gatineau, Quebec, specializing in criminal law, as disciplinary court chairperson in federal penitentiaries and also as defending officer for courts martial. Thereafter, Mr. Plouffe worked for the Legal Aid Office as office director of the criminal law section.

Mr. Plouffe was appointed a reserve force military judge in 1980, and then as a judge of the Quebec Court in 1982. For several years, he was a lecturer in criminal procedure at the University of Ottawa Civil Law Section. He was thereafter appointed to the Superior Court of Quebec in 1990, and to the Court Martial Appeal Court of Canada in March 2013. He retired as a supernumerary judge on April 2, 2014.

During his career, Mr. Plouffe has been involved in both community and professional activities. He has received civilian and military awards.

ANNEX B: EXCERPTS FROM THE *NATIONAL DEFENCE ACT* AND THE *SECURITY OF INFORMATION ACT* RELATED TO THE COMMISSIONER'S MANDATE

NATIONAL DEFENCE ACT – PART V.1

Appointment of Commissioner

273.63

(1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

Duties

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

Annual report

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

Powers of investigation

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

Employment of legal counsel, advisers, etc.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

Directions

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

...

Review of authorizations

273.65

(8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

SECURITY OF INFORMATION ACT

Public interest defence

15.

(1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest.

...

Prior disclosure to authorities necessary

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following:

(a) the person has, before communicating or confirming the information, brought his or her concern ... to his or her deputy head or ... the Deputy Attorney General of Canada; and

(b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, ...

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.